

WHAT IS CLAIMED IS:

Sub
A3

5 1. A portable unit comprising:
storage means for storing registration data; and
encryption means for encrypting the registration
data stored in said storage means in executing personal
authentication based on the registration data and new
input information, and supplying the obtained cipher to
a personal authentication unit which is communicatively
connected to said portable unit and executes the
10 personal authentication.

2. A unit according to claim 1, wherein the
registration data is personal biological data.

15 3. A unit according to claim 1, wherein said
unit further comprises random number generating means
for generating a random number when the personal
authentication is to be executed, and said encryption
means comprises means for supplying, to said personal
authentication unit, a ciphertext obtained by
encrypting the registration data with a random number
20 generated by said random number generating means and
a ciphertext obtained by encrypting the random number
with a key held by said personal authentication unit.

25 4. A personal authentication unit having tamper
resistance, comprising:
tamper-resistant decryption means for obtaining
registration data by decrypting a ciphertext supplied
from a portable unit for storing the registration data

09506377, 021300

and outputting the ciphertext obtained by encrypting the registration data;

input means for inputting input information; and

collation means for collating the registration

5 data obtained from said decryption means with the input information input from said input means.

5. A portable unit comprising:

means for storing registration data; and

encryption means for, in executing a personal

10 authentication based on the registration data

and new input information, supplying a ciphertext

obtained by encrypting the registration data stored in

the said storage means to a fixed section which is

communicatively connected to said portable unit and

15 performs transfer processing including encryption

between said portable unit and a plurality of personal

authentication units for performing personal

authentication.

20 6. A personal authentication system having tamper resistance, comprising:

a tamper-resistant fixed section including:

first tamper-resistant decryption means for

obtaining registration data by decrypting a ciphertext

supplied from a portable unit for storing the

25 registration data and outputting the ciphertext

obtained by encrypting the registration data;

encryption means for sending a ciphertext obtained

09506377, 021800

by encrypting the registration data obtained from
said first decryption means with a predetermined
cryptographic key;

5 a plurality of tamper-resistant personal
authentication units each of which is movably
installed;

10 second decryption means for obtaining registration
data by decrypting the ciphertext sent from said
decryption means with a predetermined cryptographic
key; and

collation means for collating the registration
data obtained from said second decryption means with
the input information.

15 7. A computer readable medium used for
a tamper-resistant portable unit which can communicate
with a personal authentication unit for executing
personal authentication and includes a computer, said
medium storing a program for

20 causing said computer to execute a procedure for
storing registration data in storage means; and

causing said computer to execute an encryption
procedure for encrypting the registration data and
supplying the obtained ciphertext to said personal
authentication unit when executing the personal
25 authentication.

8. A computer readable medium used for
a tamper-resistant personal authentication

09506377-021800

unit having a computer and executing a personal authentication on the basis of a ciphertext supplied from a tamper-resistant portable unit for storing registration data and outputting a ciphertext obtained by encrypting the registration data, said medium
5 storing a program for

causing said computer to execute a decryption procedure for obtaining registration data by decrypting the ciphertext supplied from said portable unit;

10 causing said computer to execute an input procedure for inputting input information; and

causing said computer to execute a collation procedure for collating the registration data obtained by the decrypt procedure with the input information.

15 9. A computer readable medium used for a tamper-resistant portable unit having a computer and capable of communicating with a personal authentication system including a tamper-resistant fixed section which has a computer and obtains
20 registration data by decrypting a ciphertext supplied from a tamper-resistant portable unit for storing registration data and outputting a ciphertext obtained by encrypting the registration data, encrypts the
25 obtained registration data by using a predetermined cryptographic key, and transfers the ciphertext to a plurality of personal authentication units for executing personal authentication, and said plurality

09506377 024800

of tamper-resistant personal authentication units each
of which has a computer, decrypts the ciphertext from
said fixed section, and collates obtained information
with input information, thereby executing a personal

5 authentication, said medium storing a program for

causing said computer to execute a procedure for
storing registration data; and

causing said computer to execute an encryption
procedure for supplying the ciphertext obtained by
10 encrypting the registration data to said fixed section
when executing the personal authentication.

10. A computer readable medium used for a personal
authentication system including a tamper-resistant
fixed section which has a computer and obtains
15 registration data by decrypting the ciphertext supplied
from a tamper-resistant portable unit for storing
registration data and outputting a ciphertext obtained
by encrypting the registration data, encrypts the
obtained registration data by using a predetermined
20 cryptographic key, and transfers the ciphertext to
a plurality of personal authentication units for
executing personal authentications, and said plurality
of tamper-resistant personal authentication units each
of which has a computer, decrypts the ciphertext from
25 said fixed section, and collates obtained information
with input information, thereby executing a personal
authentication, said medium storing a program for

003720 77690560

causing said computer of said fixed section to execute a first decryption procedure for obtaining registration data by decrypting a ciphertext supplied from said portable unit;

5 causing said computer to execute a second encrypt procedure for encrypting the registration data obtained by the first decryption procedure with a predetermined cryptographic key and sending the obtained ciphertext;

10 causing said computer of each of said personal authentication units to execute a second decryption procedure for obtaining registration data by decrypting the ciphertext sent by the second encryption procedure with a predetermined cryptographic key; and

15 causing said computer to execute a collation procedure for collating the registration data obtained by the second decrypt procedure with the input information.

11. A personal authentication system comprising:

a tamper-resistant portable unit including:

20 a memory for storing registration data;
encryption means for, when a personal authentication is to be executed, encrypting the registration data stored in said memory;

25 supply means for supplying the registration data encrypted by said encryption means to a personal authentication unit;

a tamper-resistant personal authentication unit

09506377 021800

capable of communicating with said portable unit,
including:

input means for inputting registration data;

decryption means for decrypting the encrypted

5 registration data supplied from said supply means; and

collation means for collating the registration
data decrypted by said decryption means with the
registration data input by said input means.

10 12. A system according to claim 11, wherein said
portable unit and said personal authentication unit
further comprise authentication means for performing
mutual authentication between said portable unit and
said personal authentication unit.

15 13. A system according to claim 12, wherein said
authentication means respectively have certificates
and private keys and execute verification of
the certificates and mutual authentication of
authenticating information indicating that said unit
and said unit mutually have the private keys.

20 14. A system according to claim 13, wherein
said portable unit verifies the certificate of
said personal authentication unit by decrypting
a signature of an authentication office which is
contained in the certificate received from said
25 personal authentication unit by using a public key of
the authentication office, and performing true-false
determination of the decryption result by using a name

008120 2250560

of the authentication office.

15. A system according to claim 11, wherein the input information collated by said collation means is personal biological information.

5 16. A portable unit used for said personal authentication system defined in claim 11, comprising:

random number generating means for generating a random number when the personal authentication is to be executed; and

10 encryption means for generating a first ciphertext by encrypting the registration data with the random number generated by said random number generating means, generating a second ciphertext by encrypting the random number by using a key obtained from said personal authentication unit, and supplying the first and second
15 ciphertexts to said personal authentication unit.

17. An article of manufacture comprising:

a computer readable medium having computer readable program code means embodied therein for
20 causing a personal authentication to be performed between a portable unit and a personal authentication unit, the computer program code means in said article of manufacturing comprising:

computer readable program code means for causing
25 a computer to encrypt, when the personal authentication is to be performed, the registration data and to supply the encrypted registration data to the personal

09506377.021800

authentication unit;

computer readable program code means for causing the computer to decrypt the encrypted data to obtain the registration data;

5 computer readable program code means for causing the computer to input registration data; and

computer readable program code means for causing the computer to collate the registration data obtained by the decryption with the inputted registration data.

10 18. A personal authentication system comprising:

a tamper-resistant portable unit including:

a memory for storing registration data;

15 a tamper-resistant fixed section containing a plurality of personal authentication units for performing encryption and transfer processing between said portable unit and said plurality of personal authentication units;

20 first encryption means for supplying a ciphertext obtained by encrypting the registration data stored in said memory to said fixed section;

the said fixed section including:

first decryption means for obtaining registration data by decrypting the ciphertext supplied from said first encryption means; and

25 second encryption means for encrypting the registration data obtained by said first decrypting means with a predetermined cryptographic key, and

008720 7690550

sending the obtained ciphertext;

said plurality of personal authentication units having tamper-resistance is capable of executing personal authentications on the basis of the registration data in said portable unit and new input information, each of said personal authentication units including:

second decryption means for obtaining registration data by decrypting the ciphertext sent from said second encryption means with a predetermined cryptographic key; and

collation means for collating the registration data obtained by said second decryption means with the input information.

19. A portable unit used for said personal authentication system defined in claim 18, comprising:

random number generating means for generating a random number when the personal authentication is to be executed; and

first encryption means for supplying, to said fixed section, a ciphertext obtained by encrypting the registration data with the random number generated by said random number generating means and a ciphertext obtained by encrypting the random number with a key of said fixed section.

008120 22E90560